情報ネットワーク学 期末レポート

技術系経営戦略学専攻 M1 37-176839 田村浩一郎

テーマ: AI とサイバーテロ対策

1. テーマの概要と具体例

情報漏洩やサイバー攻撃などといった問題は，個人や企業という枠組みだけでなく，国家間同士でおこっている問題である．例えば，ロシアがアメリカにサイバー攻撃を仕掛け，トランプ大統領がその事実を認めた[1]という話題は有名である．また，スウェーデン政府が誤ってほぼ全国民の個人情報に加え，軍の機密事項まで漏洩してしまったというニュース[2]も記憶に新しい．これらの問題は，ただ技術的な問題であるというわけではないが，次世代ファイアーウォール，IDS/IPS，WAF，Web フィルタリング，アンチウイルスなど様々な対策試みられている．さらに近年，AI を用いたサイバーテロ対策が話題になっており，本レポートでは AI によるサイバーテロ対策に着目した．

AI によるサイバーテロ対策は，具体的には，ビックデータを用いた異常検知を行うことである．サイバーテロ以外にも，ビックデータを用いたリスク検知といった分野は注目されており，近年だと株式会社エルテス[3]がそういった事業に取り組み，投資家を沸かせた．サイバーテロ対策で言えば，MIT（マサチューセッツ工科大学）のコンピュータ科学および人工知能研究所が、開発したサイバー攻撃検知システム[4]や，ソフトバンクが出資した米国ベンチャー企業のサイバーリーズ社によるサイバー攻撃対策[4]，NTT コミニケーションが開発した不審な通信を自動検知して遮断するシステム[4]などがある．

2. テーマに対する自分の意見

AI 技術が大きなブレイクスルーとなっている今，異常検知という枠組みで AI 技術をサイバー攻撃，サイバーテロの対抗策として用いるトレンドは今後ますます盛んになってくると考えられる．また，上記の例では企業単位の対策が行われていることを示したが，こうした企業と国が連携したり，国で専門の機関を保有するなど，国家レベルでの対策を早く講じるべきである．断片的な技術や情報を集積し，自律的に情報管理を行う国家システムが必要である．例えば，マルウェア感染対策では，マルウェアの異常検知だけでなく，ユーザーの log データなどから元に，潜在的にマルウェアに感染しやすいユーザーを事前に特定するといったことが考えられる．

そういった意味では，今後 IoT の流行は一つの鍵になるだろう．授業で学習したように，

IoT のように多くの機器がオンラインになることでネットワークにおける感染リスクが高まる可能性もあるが, IoT の発展によって集積されたデータを用いてより高度で正確な異常検知をすることができれば, サイバーテロ対策, さらにはもっと大きな枠組みでリスク管理をすることができるはずである.

[参考]

[1] http://www.newsweekjapan.jp/stories/world/2017/01/post-6694_1.php

[2]https://www.thelocal.se/20170717/swedish-authority-handed-over-keys-to-the-kingdom-in-it-security-slip-up

[3] https://eltes.co.jp/

[4] http://it-trend.jp/cyber_attack/article/use_of_ai